In the Claims:

[c1] 1. A network apparatus, connected to other network entities via a first type of connection and other network entities via a second type of connection, comprising:

a spoofing element, which spoofs some of the multiple connections of the first type based on their associated applications.

[c2] 2. The network apparatus of claim 1, wherein said spoofing element only spoofs connections of the first type associated with high throughput applications.

[c3] 3. The network apparatus of claim 1, wherein said spoofing element assigns spoofing resources, including buffer space and control blocks, to the spoofed connections.

[c4] 4. The network apparatus of claim 1, wherein said spoofing element spoofs connections using at least one spoofing rule based on destination address, source address, destination port number, source port number, options, a differentiated services (DS) field or combinations thereof.

[c5] 5. The network apparatus of claim 4, wherein said spoofing element defines the at least one spoofing rule in a selective spoofing profile.

[c6] 6. The network apparatus of claim 1, wherein said spoofing element assigns at least one spoofing parameter set, including at least one of maximum transmission unit (MTU), maximum segment size (MSS), three-way handshake spoofing, connection priority, maximum advertised window size, response (or retransmission) timeout, number of retransmissions, fast retransmission threshold, keep alive timeout, retry counts, retransmission timeouts, and initial window sizes, or combinations thereof to the spoofed connections based on the type of application.

[c7] 7. The network apparatus of claim 6, wherein said spoofing element selects parameters for a spoofed connection using at least one spoofing rule based on destination address, source address, destination port number, source port number, options, a differentiated services (DS) field or combinations thereof.

[c8] 8. The network apparatus of claim 7, wherein said spoofing element defines the at least one spoofing rule in a selective spoofing profile.

[c9] 9. The network apparatus of claim 6, wherein said spoofing element defines the at least one spoofing parameter set in a spoofing parameter profile.

[c10] 10. The network apparatus of claim 1, wherein said spoofing element spoofs some of the multiple connections of the first type based on at least one operator selectable criterion.

[c11] 11. The network apparatus of claim 1, wherein said spoofing element selects parameters for spoofing some of the multiple connections of the first type based on at least one operator selectable criterion.

[c12] 12. The network apparatus of claim 1, wherein the first connection uses a high layer protocol.

[c13] 13. The network apparatus of claim 12, wherein the first connection uses one of the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

[c14] 14. The network apparatus of claim 1, wherein the second connection is a backbone connection.

[c15] 15. The network apparatus of claim 14, wherein the backbone connection is via a wireless link.

[c16] 16. The network apparatus of claim 15, wherein the wireless link has high latency and high error rate.

[c17] 17. The network apparatus of claim 15, wherein the wireless link is a satellite link.

[c18] 18. The network apparatus of claim 1, wherein said network apparatus is a component of a network gateway.

[c19] 19. The network apparatus of claim 1, wherein said network apparatus is a component of a host.

[c20] 20. The network apparatus of claim 1, wherein said network apparatus is a component of a hub.

[c21] 21. The network apparatus of claim 1, wherein said network apparatus is a component of a switch.

[c22] 22. The network apparatus of claim 1, wherein said network apparatus is a component of a VSAT.

[c23] 23. The network apparatus of claim 1, wherein said network apparatus is a component of a router.

[c24] 24. A method, comprising:

establishing multiple connections of a first type associated with different applications; and

spoofing some of the multiple connections of the first type based on their associated applications.

[c25] 25. The method of claim 24, wherein said spoofing step only spoofs connections of the first type associated with high throughput applications.

[c26] 26. The method of claim 24, wherein said spoofing step assigns spoofing resources, including buffer space and control blocks, to the spoofed connections.

[c27] 27. The method of claim 24, wherein said spoofing step spoofs connections using at least one spoofing rule based on destination address, source address, destination port number, source port number, options, a differentiated services (DS) field or combinations thereof.

[c28] 28. The method of claim 27, wherein said spoofing step defines the at least one spoofing rule in a selective spoofing profile.

[c29] 29. The method of claim 24, wherein said spoofing step assigns at least one spoofing parameter set, including at least one of maximum

transmission unit (MTU), maximum segment size (MSS), three-way handshake spoofing, connection priority, maximum advertised window size, response (or retransmission) timeout, number of retransmissions, fast retransmission threshold, keep alive timeout, retry counts, retransmission timeouts, and initial window sizes, or combinations thereof to the spoofed connections based on the type of application.

[c30] 30. The method of claim 29, wherein said spoofing step selects parameters for a spoofed connection using at least one spoofing rule based on destination address, source address, destination port number, source port number, options, a differentiated services (DS) field or combinations thereof.

[c31] 31. The method of claim 30, wherein said spoofing step defines the at least one spoofing rule in a selective spoofing profile.

[c32] 32. The method of claim 29, wherein said spoofing step defines the at least one spoofing parameter set in a spoofing parameter profile.

[c33] 33. The method of claim 24, wherein said spoofing step spoofs some of the multiple connections of the first type based on at least one operator selectable criterion.

[c34] 34. The method of claim 24, wherein said spoofing step selects parameters for spoofing some of the multiple connections of the first type based on at least one operator selectable criterion.

[c35] 35. The method of claim 24, wherein the first connection uses a high layer protocol.

[c36] 36. The method of claim 35, wherein the first connection uses one of the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

[c37] 37. The method of claim 24, wherein said method is performed in a network gateway.

[c38] 38. The method of claim 24, wherein said method is performed in a host.

[c39] 39. The method of claim 24, wherein said method is performed in a hub.

[c40] 40. The method of claim 24, wherein said method is performed in a switch.

[c41] 41. The method of claim 24, wherein said method is performed in a VSAT.

[c42] 42. The method of claim 24, wherein said method is performed in a router.